(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/92982 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/IL01/00489

(22) International Filing Date: 29 May 2001 (29.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/207,927 30 May 2000 (30.05.2000) US

(71) Applicant and
(72) Inventor: CASPI, Moshe [IL/IL]; No. 75, 99750 Zelafon (IL).

(74) Agent: MILLER - SIERADZKI ADVOCATES & PATENT ATTORNEYS; P.O. Box 6145, 31061 Haifa (IL).

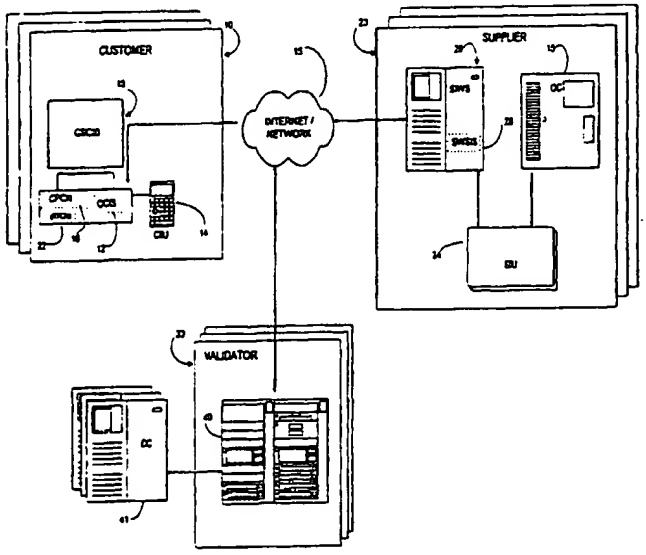
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR SECURE TRANSACTIONS VIA A COMMUNICATIONS NETWORK



(57) Abstract: A method and a system for facilitating online commerce between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device. Security-sensitive input/output operations are carried out at each end of the transaction by dedicated computing means, one for the customer and one for the supplier. The dedicted customer computing means is communication-connected to the customer computing device and the supplier's dedicted computing means is communication-connected to the supplier's e-commerce server and order-processing computer (separate connections). Encrypted messages pass between the dedicated devices via a validating third party. The tasks handled are: requesting customer confirmation; executing payment upon confirmation; and supplying goods or services.

WO 01/92982 A2

THIS PAGE BLANK (USPTO)

SYSTEM AND METHOD FOR SECURE TRANSACTIONS VIA A COMMUNICATIONS NETWORK

FIELD OF THE INVENTION

The present invention relates to network data communications. More particularly, it relates to ensuring the security of transactions conducted over a communications network.

BACKGROUND OF THE INVENTION

Transactions carried out via a communications network must be protected from access by unauthorized parties. The protection must extend to the computers of both parties conducting the transaction as well as the communications network itself. A common example of such a transaction is where a customer purchases a good or service from a supplier's Web site, in other words an e-commerce transaction.

The e-commerce transaction is vulnerable to any number of malicious interference on the part of unauthorized intruders, referred to herein as hackers. Some examples: A hacker can conduct an illegal transaction on the supplier Web site by remotely manipulating a legitimate customer's computer without that customer being aware of his doing so or by impersonating the customer after surreptitiously learning the customer's identification code or credit card number. Similarly a hacker can penetrate the supplier's Web site, sending bogus information to the customer or intercepting the customer's payment. In other words, the hacker can interfere with the information transferred between the two parties to the transaction, particularly regarding what the customer thinks he is buying, what the supplier thinks the customer is buying, whether the customer approves payment, and whether payment is received by the supplier.

To protect against these and other illegal activities, the customer computer, the supplier Web site server computer, and the communications link must be made secure. The only way to guarantee 100% security for such a client-server architecture would be to create a completely closed system. This is almost never practical. In fact computers are built for flexibility and Internet protocols are designed for universality.

Attempts have been made to improve security, but the solutions offered to date have only been partial in nature, protecting either the communication line or the computers themselves. Moreover, these partial solutions are usually expensive and require technical expertise. Presently, no single system exists that provides an all- encompassing, affordable, easy-to-use solution to the problem of securing electronic transactions, particularly via the Internet.

For example, software has been developed to encrypt the data transmitted between the customer's and supplier's computers, but this only protects against data interception on the communication line. Both the customer's and supplier's computers remain exposed to hackers who can potentially access information stored on them.

Another solution has been to use a hardware interface in the customer's computer that can identify the computer and verify its identification to the supplier's computer. This solution does not adequately address the problem of hackers penetrating the customer computer's software through which the computer's input and output functions.

US patent 5,883,810, awarded in 1999 to Franklin et al, and entitled "Electronic online commerce card with transaction proxy number for online transactions," describes an online commerce system where an issuing institution generates a temporary transaction number for a customer and associates it with the customer's permanent account number in a data record. The customer submits the transaction number to the merchant as a proxy for the customer account number. The merchant handles the transaction number in the same manner as any regular credit card number. When the merchant asks the issuing institution for verification, the issuing institution references the customer account number, using the transaction number as an index, processes the authorization request using the real customer account number in place of the proxy number, and sends an authorization reply back to the merchant under the transaction number.

This system still does not prevent hackers from taking control of a customer's or supplier's computer either directly or via a virus-type of malicious program.

US patent no. 5,524,072, awarded in 1996 to Labaton et al, entitled "Methods and apparatus for data encryption and transmission" provides a portable hand-held module having the confidential data and a predetermined encryption algorithm embedded therein. The apparatus which receives the encrypted transmission is equipped with an interface computer having decryption circuitry in which the inverse of the forgoing encryption algorithm is embedded.

The module includes input means for the customer to enter his order and a DTMF tone generator for communicating the customer order and ID number to a computer via that computer's microphone. While the tone generation is compatible with some aspects of telephony, it is limited for use with computers since it is unidirectional - from the customer to the computer. Furthermore, the customer is required to reenter transaction details himself as part of the confirmation process. This is tedious for the customer and creates the possibility of errors creeping in.

In addition, this system does not include any dedicated secure device for the supplier side of the transaction, nor does it provide for third party validation of the transaction, nor is their a mechanism for verifying that the information presented to the customer is valid.

The present invention is unique in that it is designed to provide full, affordable, easy-to-use security for electronic transactions. It completely prevents hackers from using the customer and supplier computers to access the critical parts of the transaction. This is accomplished by moving these parts, including encryption/decryption, out of the computers and into dedicated external computing devices. The external devices are connected to the computers via a secure communications protocol that limits the computer's access to the device to only predefined functions. No transaction is completed until the customer has approved it via the user input means of his external computing device. Therefore, it is physically impossible for a remote hacker to carry out an unauthorized transaction.

Another advantage of the present invention is that any or all parts of the invention can be fully automated, operating without human intervention.

The preferred embodiment of the present invention applies to e-commerce transactions via the Internet. The same principles can be applied in alternative embodiments for other forms of data transactions on other types of communications networks.

BRIEF DESCRIPTION OF THE INVENTION

There is thus provided in accordance with a preferred embodiment of the present invention, a method for facilitating online commerce between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device, the method comprising the following steps:

a providing the customer with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device and having user input/output means, the customer's dedicated computing means communicating with the customer computing device; and

b providing the supplier with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device, the supplier's computing means communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing means; and

c requesting customer confirmation; and

d executing payment upon confirmation; and

e supplying goods or services,

thereby facilitating online commerce between a customer and a supplier.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the requesting customer confirmation step comprises the following steps:

a initially validating the customer order on the supplier's order-filling computing means;

b encrypting the order with supplier's private code and sending a payment request to the validating computing device;

c decrypting the order, encrypting with user's private code and sending to customer's dedicated computing means;

d decrypting the order and outputting it to the customer;

e the customer inputting his or her confirmation;

f encrypting the confirmation and sending to the validating computing device;

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the executing payment upon confirmation step comprises the following steps:

a decrypting the customer confirmation;

b notifying the customer's payment provider to execute payment;

c receiving confirmation of payment from said payment provider;

d encrypting payment confirmation and sending to supplier's dedicated computing means;

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the supplying goods or services step comprises the following steps:

a decrypting the payment confirmation;

b notifying supplier's order-filling computing means to execute order;

c filling order by providing goods or services to customer.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the supplier's order-filling computing means performs the further check of comparing order as confirmed with original order.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the method is carried out automatically.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the requesting customer confirmation step, the executing payment upon confirmation step, and the supplying goods or services step are all carried out online.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the method is carried out over the Internet

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the method is carried out over an intranet

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the transaction is initiated at an e-commerce Web site.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the method is carried out automatically.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the validating computing device maintains a copy of the transaction.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the validating computing device maintains a database about the transaction.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that all encrypted messages for a given order have a unique identifier known and checked by the supplier's order-filling computing means.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer's dedicated computing means is a stand-alone device.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer's dedicated computing means is integrated into a remote control unit, the customer's computing device is a Web-enabled television set, and the two are connected via a bidirectional communications means.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer's dedicated computing means is an electronic commerce card;

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the supplier's dedicated computing means is a stand-alone device.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer's dedicated computing means is provided with user access protection means.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer input means on the customer's dedicated computing means is touch-based, as in a keyboard, keypad, or touchscreen and appropriate software.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer input means on the customer's dedicated computing means is voice-based, as in a microphone and voice recognition software.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the means for output to the customer on the customer's dedicated computing means is display-based, as in an alpha-numeric or graphical display and appropriate software.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the means for output to the customer on the customer's dedicated computing means is to a port, as in a parallel port to a printer.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the means for output to the customer is to a printer integrated into the customer means.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer has a public identification code.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the validating computing device provides the customer's dedicated computing means with an anonymous identification code.

There is thus also provided in accordance with a preferred embodiment of the present invention, at a customer conducting an online transaction, a method for handling an order confirmation request from a validating computing device, comprising the following steps:

a providing the customer with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device and having user input/output means, the customer's dedicated computing means communicating with the customer computing device;

b the dedicated computing means receiving an encrypted confirmation request from the validating computing device;

c decrypting the order and outputting it to the customer;

d the customer inputting his or her confirmation;

e encrypting the confirmation and sending to the validating computing device;

There is thus also provided in accordance with a preferred embodiment of the present invention, at a supplier conducting an online transaction, a method for working with a validating computing device and an order-filling computing means to confirm, bill, and fill a customer order, comprising the following steps:

a providing the supplier with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device, the supplier's computing means communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing means;

b initially validating the customer order on the supplier's order-filling computing means;

c encrypting the order with supplier's private code and sending payment request to the validating computing device;

d decrypting payment confirmation received from validating computing device;

e notifying supplier's order-filling computing means to execute order;

f filling order by providing goods or services to customer.

There is thus also provided in accordance with a preferred embodiment of the present invention, a method for facilitating online transactions between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device, the method comprising the following steps:

a providing the customer with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device and having user input/output means, the customer's dedicated computing means communicating with the customer computing device;

b providing the supplier with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device, the supplier's computing means communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing means;

c requesting customer confirmation, comprising the following steps:

i initially validating the customer order on the supplier's order-filling computing means;

ii encrypting the order with supplier's private code and sending a payment request to the validating computing device;

iii decrypting the order, encrypting with user's private code and sending to customer's dedicated computing means;

iv decrypting the order and outputting it to the customer;

v the customer inputting his or her confirmation;

vi encrypting the confirmation and sending to the validating computing device;

d executing payment upon confirmation, comprising the following steps:

i initially validating the customer order on the supplier's order-filling computing means;

ii decrypting the customer confirmation;

iii notifying the customer's payment provider to execute payment;

iv receiving confirmation of payment from said payment provider;

v encrypting payment confirmation and sending to supplier's dedicated computing means;

a) and supplying the goods or services, comprising the following steps:

i decrypting the payment confirmation;

ii notifying supplier's order-filling computing means to execute order;

iii filling order by providing goods or services to customer.

There is thus also provided in accordance with a preferred embodiment of the present invention, a system for facilitating online transactions between a customer's computer device and a supplier's computing device, in cooperation with a validating computing device, the system comprising the following:

a a dedicated customer computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device and having user input/output device, the customer's dedicated computing device communicating with the customer computing device and programmed to receive an order confirmation request, decrypt the request, output the request to the user (customer), receive the customer's response (input) to the confirmation request, encrypt the customer response; and send the response to the validating computing device;

b a dedicated supplier computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device, the supplier's computing device communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing device and programmed to receive a customer order from the supplier's transaction site, encrypt an order and payment confirmation request, send the request to the validating computing device; receive order and payment confirmed message from the validating computing device, and notify the order-filling computing device to fill the order.

c the validating computing device being configured to receive an order and payment confirmation request from the dedicated supplier computing device, decrypt the request, encrypt an order confirmation request for the customer, send the request to the customer, receive the customer's response, decrypt the response, notify the customer's payment provider to execute payment, receive confirmation of payment from said payment provider; encrypt an order and payment confirmed message, and send said message to the dedicated supplier computing device.

There is thus also provided in accordance with a preferred embodiment of the present invention, a system for facilitating online commerce between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device, the system comprising the following:

a providing the customer with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device and having user input/output device, the customer's dedicated computing device communicating with the customer computing device; and

b providing the supplier with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device, the supplier's computing device communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing device; and

c requesting customer confirmation; and

d executing payment upon confirmation; and

e supplying goods or services.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the confirmation comprises the following:

a initially validating the customer order on the supplier's order-filling computing device;

b encrypting the order with supplier's private code and sending a payment request to the validating computing device;

c decrypting the order, encrypting with user's private code and sending to customer's dedicated computing device;

d decrypting the order and outputting it to the customer;

e the customer inputting his or her confirmation;

f encrypting the confirmation and sending to the validating computing device;

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that executing payment upon confirmation comprises the following:

a decrypting the customer confirmation;

b notifying the customer's payment provider to execute payment;

c receiving confirmation of payment from said payment provider;

d encrypting payment confirmation and sending to supplier's dedicated computing device;

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the supplying goods or services comprises the following:

a decrypting the payment confirmation;

b notifying supplier's order-filling computing device to execute order;

c filling order by providing goods or services to customer.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the supplier's order-filling computing device performs the further check of comparing order as confirmed with original order.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the system is automatic.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the requesting customer confirmation, the executing payment upon confirmation, and the supplying goods or services are all carried out online.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the system is implemented over the Internet.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the system is implemented over an intranet.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the validating computing device maintains a copy of the transaction.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the validating computing device maintains a database about the transaction.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that all encrypted messages for a given order have a unique identifier known and checked by the supplier's order-filling computing device.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the transaction is initiated at an e-commerce Web site.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the system is carried out automatically.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer's dedicated computing device is a stand-alone device.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer's dedicated computing device is integrated into a remote control unit, the customer's computing device is a Web-enabled television set, and the two are connected via a bidirectional communications device.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer's dedicated computing device is an electronic commerce card;

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the supplier's dedicated computing device is a stand-alone device.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer's dedicated computing device is provided with user access protection device.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer input device on the customer's dedicated computing device is touch-based, as in a keyboard, keypad, or touchscreen and appropriate software.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer input device on the customer's dedicated computing device is voice-based, as in a microphone and voice recognition software.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the device for output to the customer on the customer's dedicated computing device is display-based, as in an alpha-numeric or graphical display and appropriate software.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the device for output to the customer on the customer's dedicated computing device is to a port, as in a parallel port to a printer.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the device for output to the customer is to a printer integrated into the customer device.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the customer has a public identification code.

Furthermore, in accordance with another preferred embodiment of the present invention, further comprising that the validating computing device provides the customer's dedicated computing device with an anonymous identification code.

There is thus also provided in accordance with a preferred embodiment of the present invention, at a customer conducting an online transaction, a system for handling an order confirmation request from a validating computing device, comprising the following :

a providing the customer with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device and having user input/output device, the customer's dedicated computing device communicating with the customer computing device;

b the dedicated computing device receiving an encrypted confirmation request from the validating computing device;

c decrypting the order and outputting it to the customer;

d the customer inputting his or her confirmation;

e encrypting the confirmation and sending to the validating computing device;

There is thus also provided in accordance with a preferred embodiment of the present invention, at a supplier conducting an online transaction, a system for working with a validating computing device and an order-filling computing device to confirm, bill, and fill a customer order, comprising the following :

a providing the supplier with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device, the supplier's computing device communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing device;

b initially validating the customer order on the supplier's order-filling computing device;

c encrypting the order with supplier's private code and sending payment request to the validating computing device;

d decrypting payment confirmation received from validating computing device;

e notifying supplier's order-filling computing device to execute order;

f filling order by providing goods or services to customer.

There is thus also provided in accordance with a preferred embodiment of the present invention, a system for facilitating online transactions between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device, the system comprising the following :

a providing the customer with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device and having user input/output device, the customer's dedicated computing device communicating with the customer computing device;

b providing the supplier with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device, the supplier's computing device communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing device;

c requesting customer confirmation, comprising the following:

i initially validating the customer order on the supplier's order-filling computing device;

ii encrypting the order with supplier's private code and sending a payment request to the validating computing device;

iii decrypting the order, encrypting with user's private code and sending to customer's dedicated computing device;

iv decrypting the order and outputting it to the customer;

v the customer inputting his or her confirmation;

vi encrypting the confirmation and sending to the validating computing device;

d executing payment upon confirmation, comprising the following:

i initially validating the customer order on the supplier's order-filling computing device;

ii decrypting the customer confirmation;

iii notifying the customer's payment provider to execute payment;

iv receiving confirmation of payment from said payment provider;

v encrypting payment confirmation and sending to supplier's dedicated computing device;

e and supplying the goods or services, comprising the following:

i decrypting the payment confirmation;

ii notifying supplier's order-filling computing device to execute order;

iii filling order by providing goods or services to customer.

BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 is a general block diagram of a system for secure electronic transactions in accordance with a preferred embodiment of the present invention.

FIG. 2A is a block diagram of a dedicated customer computing device for secure electronic transactions integrated into a bidirectional remote control unit of a Web-enabled television set in accordance with an alternative embodiment of the present invention.

FIG. 2B is a block diagram of a dedicated customer computing device for secure electronic transactions with a second communications port connected to an external printer in accordance with an alternative embodiment of the present invention.

FIG. 3A is the first part of a flowchart showing the operation of a system for secure electronic transactions in accordance with a preferred embodiment of the present invention.

FIG. 3B is the second part of a flowchart showing the operation of a system for secure electronic transactions in accordance with a preferred embodiment of the present invention.

FIG. 3C is the third part of a flowchart showing the operation of a system for secure electronic transactions in accordance with a preferred embodiment of the present invention.

FIG. 3D is the fourth part of a flowchart showing the operation of a system for secure electronic transactions in accordance with a preferred embodiment of the present invention.

FIG. 3E is the fifth part of a flowchart showing the operation of a system for secure electronic transactions in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The preferred embodiment of the present invention comprises a number of hardware and software components. When a component is introduced in this detailed description, its full name and acronym are given. Thereafter the acronym is used in the description and in the drawings. The components, acronyms and reference numbers are also listed below.

REF. NO.	ACRONYM	FULL DESCRIPTION
10		- Customer
12	CCIS	- Customer Computer Interface Software.
14	CIU	- Customer Interface Unit.
16	CPCN	- Customer Public Code Number.
18	CSCIB	- Customer Standard Computer with Internet Browser
20	OC	- Order Computer.
22	RTCN	- Random Transaction Code Number.
23		- Supplier
24	SIU	- Supplier Interface Unit.
26	SIWS	- Supplier Internet Web Site
28	SWSIS	- Supplier Web Site Interface Software.
39		- Validator
40	VC	- Validation Computer
41	BC	- Bank Computer

Reference is now made to FIG. 1, which is a block diagram of a system and method for secure data transactions over a communications network in accordance with a preferred embodiment of the present invention.

The system is based on three primary entities: a Customer 10, who initiates the transaction, a Supplier 23, who provides a good, service, or other benefit to the Customer, and a Validator 39 who acts as an intermediary between the two for purposes of validating and processing confidential information, such as the identity of the Customer and payment execution. A fourth entity is a bank or other payment authority, which is executes payment from Customer 10 to Supplier 23, upon request by Validator 39.

Both the Customer 10 and the Supplier 23 have a dedicated computing device for conducting sensitive steps in the transaction. Each of these dedicated computing devices has a private key and a public ID number. The private key is known only to the dedicated computing device and to the Validator 39.

The Validator 39 is the entity that maintains a record of the keys of the two types of dedicated computing devices. A device's key could typically be embedded by the Validator before distributing the device to a Customer 10 or Supplier 23. Upon purchase or installation of the device, the Customer 10 or Supplier 23 would register himself with the Validator 39. Or other methods and systems known to those familiar with the art can be used to embed the private keys and register the Customer 10 and Supplier 23 with the Validator 39.

The present invention involves encrypted messages sent over a secure channel. In the preferred embodiment described herein, decryption is accomplished using public and private keys. Other methods and systems could equally be used to achieve this functionality, such as doing without public keys and instead having the decrypting device simply try every private key until it finds the correct one.

It is a major purpose of the present invention to enable Customer and Supplier to carry out encryption/decryption procedures and sensitive input/output procedures on their respective dedicated computing devices, thereby eliminating access to these procedures to third parties. In particular this prevents malicious individuals from interfering with the transaction at the endpoints (Customer's Internet browser and Supplier's Web site).

The Customer 10 uses a Customer Standard Computer with an Internet Browser (CSCIB) 18. The CSCIB 18 is a computing device with Internet access (Web browsing capability) and having a local communications port (such as a serial port) 11. In the preferred embodiment of the present invention the CSCIB 18 is a personal computer but it can be any computing device with these capabilities, for example, a Web-enabled cellular phone.

In the preferred embodiment of the present invention, the customer's transaction takes place at a Supplier's Web site accessed via the Internet. Alternatively, other means for electronic commerce can be used, such as an intranet or a proprietary e-commerce application.

The Customer Interface Unit (CIU) 14 is connected to the CSCIB's 18 local communications port 11. The CIU 14 is the dedicated computing device for the Customer side of the transaction. The CIU 14 includes a means for user input, (which in the preferred embodiment is a keypad), and a means for output to the user, (which in the preferred embodiment is a display).

The CIU 14 output can alternatively, or additionally, be to a printer 15. In FIG. 2A the printer 15 is connected to a second communications port on the CIU 14. Alternatively, the printer 15 could be integrated into the CIU 14.

The CSCIB 18 software that communicates with the CIU 14 is a dedicated software module, the Customer Computer Interface Software (CCIS) 12.

The CIU 14 includes an encryption/decryption algorithm embedded with the unique private key for that particular CIU.

The CIU 14 transmits and receives encrypted messages via the CSCIB 18 and the Internet.

The CIU 14 can optionally include electronic means for identifying the Customer before allowing him access. Such means are well known, such as personal identification code, fingerprint, voice, or retinal pattern.

In the preferred embodiment of the present invention, the CIU 14 is a standalone device. Alternatively, the CIU 14 can be integrated into the CSCIB 18 or into another device, such as a cellular telephone or smart card. If the CIU 14 is integrated into another device, it must be implemented such that its hardware and software are independent of the rest of the device, with only a restricted communication channel connecting the two.

The primary function of the CIU 14 is to enable secure user I/O, including encryption/decryption. In the preferred embodiment of the present invention, the other operations required: messaging and browsing via the Internet, are done via the CSCIB 18.

Alternatively, the functions of the CSCIB 18 can be integrated into the CIU 14 (as separate hardware and software), or both the CIU 14 and CSCIB 18 can be integrated into a third device, such as a cellular telephone. In that case, again, the CIU 14 functionality is implemented as separate hardware and software, connecting to the rest of the device only through a limited communications channel.

FIG. 2B is an alternative embodiment of the present invention where the CIU 14 is integrated into a remote control unit for a Web-enabled television set, where the television set is used for the CSCIB 18 parts of the transaction. The communications link between the remote control unit and the television set is bidirectional.

Returning to FIG. 1, the CSCIB 18 is used by the Customer to perform the noncritical e-commerce tasks, such as item selection. However encrypted Internet messages related to the transaction are handled only by the CIU 14. For such encrypted messages the CSCIB 18 is merely a bidirectional channel, connecting to the CIU 14 the local communications port 11 at one end and to the Internet at the other end.

Encrypted transaction confirmation requests are decrypted by the CIU 14 and displayed on its display. The Customer views the information and enters his responses via the CIU's 14 keypad.

The CIU 14 encrypts the information and transmits it via the local communications port 11 of the CSCIB 18 to the Validation Center 40, as described later in this specification.

The Supplier Internet Web Site (SIWS) 26 is an e-commerce Web site running on a Web server on the Internet. The SIWS 26 has a first bidirectional communications connection 21 to an external computing device called the Supplier Interface Unit (SIU) 24. The software that manages the communication on the SIWS 26 side is referred to herein as the Supplier Web Site Interface Software SWSIS 28 module.

The SIU 24 runs an encryption/decryption algorithm embedded with a unique private key for that particular SIU 24. The SIU 24 is able to receive and transmit encrypted messages via the SIWS 26 over the Internet.

The SIU 24, in addition to having a first bidirectional communications connection 21 to the SIWS 26, has a second bidirectional communications connection 23 to one or more computing devices called the Order Computer(s) (OC) 15. The OC 15 is used to verify that the Customer has not been fooled by someone tampering with the Supplier's Web site (i.e., that the product, the price, etc. in the Customer order are identical to what is being offered on the SIWS 26). Another task of the OC 15 is to fill the order (through the Supplier's standard order fulfillment system, once Customer confirmation has been received from the VC 40 (described later) via the SIU 24. A third task of the OC 15 is to ensure that each order passing through the system has a unique identifier and then to look for that identifier in the final payment confirmation received from the VC 40. The purpose here is to keep each order processed unique and thereby prevent an unauthorized resend of a previously sent confirmation message somewhere in the system. In the preferred embodiment of the present invention, this identifier is a unique order number added by the OC 15 to the transaction details.

The tasks of the OC 15 can be done by the same OC 15 or by different OCs 15.

The SIU 24 receives transaction details from the SIWS 26, requests initial verification and unique order number from the OC 15, and after encrypting the transaction details and order number, transmits them to the Validation Center (VC) 40 via the SIWS 26 and the Internet. It will be noted that the SIU acts as a buffer between the SIWS 26, which is open to the Internet and the OC 15, which contains sensitive information.

The VC 40 is a computing device connected to the Internet that holds all Customer and Supplier private keys indexed to their public ID numbers. The VC 40 receives encrypted order messages from the SIU 24, decodes them using the Supplier's public ID number, validates them (i.e., checks that the Customer exists, that the Supplier exists, that the order meets basic criteria such as being within the Supplier's and Customer's credit range, etc.), encrypts an order confirmation request (including order number) using the Customer's private key, and sends the encrypted request to the CIU 14 via the Internet and the CSCWB 18 for Customer confirmation.

The CIU 14 decrypts the request and displays it. The Customer responds by entering his confirmation/rejection to the CIU, which the CIU 14 then encrypts (including the unique order number) using the Customer's private key and sends back to the VC 40.

In the case of a confirmation, the VC 40 contacts the bank or other payment authority 41 and requests the payment. This part of the transaction follows standard payment execution procedures, such as those used for credit card payments. Upon notification of payment, the VC 40 then encrypts a validation confirmed message (including the unique order number) using the Supplier's private key and sends it to the SIU 24. The SIU decrypts the validation message and sends the validation message to the OC 15. The OC 15, performs a final check, verifying that the unique order number is correct, then executes the transaction, e.g., ships the goods.

It is important to note that, while in the preferred embodiment of the present invention the CIU 14 and the SIU 24 are physical devices, this is not a requirement. What is a requirement is that they have the functionality defined in this disclosure. In the case of the CIU 14, this functionality consists, as mentioned, of dedicated encryption/decryption and user input/output for security-critical transaction steps, together with a limited communications channel to the CSCIB 18. The purpose being to eliminate outside access to operations performed with the CIU 14. In the case of the SIU 24, the functionality consists, as mentioned, of dedicated encryption/decryption together with a limited communications channel to the SIWS 26 and the OC 20. As long as these separate, protected functionalities are enabled, the implementation does not have to be physically separated from the other parts of the respective Customer 10 or Supplier 23 computing devices. For example, the CIU 14 could be integrated into the CSCIB 18 or into a third device, such as a cellular phone.

Reference is now made to FIG. 3A to FIG. 3E, which is a flow chart describing the operation of a system for secure data transactions over a communications network in accordance with a preferred embodiment of the present invention. The flowchart extends across the figures. The continuation of the chart from figure to figure is indicated by ending a flowchart with a letter, for example B in FIG. 3A and then starting the next flowchart with that letter (i.e., B at the top of FIG. 3B).

In step 60, a Customer uses a Customer Standard Computer with an Internet Browser (CSCIB) 18 to shop at a Supplier Internet Web Site (SIWS) 26. In step 62, he decides to purchase an item.

In step 64, the Customer selects the item and issues a purchase order (e.g., checks out his shopping cart). As part of the transaction, the Customer 10 must be identified to the Supplier 23 by his Customer Public Code Number (CPCN) 16, which can be entered by the Customer himself, taken from the CSCIB 18 as a cookie or similar automatic means, or taken from the CIU 14. If the Customer wishes to remain anonymous, he can instead use a Random Transaction Code Number (RTCN) 22, a one-time, or limited-time, code provided by the VC 40.

The idea of the RTCN 22 is to enable the Customer the option of requesting an anonymous public code from the Validation Center. For example, a Customer might want to preserve his anonymity for one or more transactions. The RTCN 22 is used in place of the CPCN 16 for the transaction. How the CIU gets the RTCN 22 can be done any number of ways. It can be done as a request from the CIU to the VC at the time of the transaction, a new RTCN 22 can be automatically maintained in a buffer in the CIU 14 by the VC, etc.

The CPCN 16 or RTCN 22 is sent by the CSCIB 18 to the SIWS 26 as part of the order. The Customer 10 may choose to send further information with the order, such as his preferred payment method, the delivery address, his e-mail address, etc. This information can be included in the order either by the customer himself, by having the CSCIB 18 supply it with a cookie or similar automatic means, or from the CIU 14.

In step 66, the order reaches the SIWS 26 where the SWSIS 28 recognizes that the order is coming from a CIU-equipped 14 Customer.

In step 68, the SWSIS 28 sends the transaction data to the OC 20 via the SIU 24.

In step 70, the OC 20 checks that the transaction accords with what is being offered on the Web site (in other words, the probability is that this is not a bogus order).

Since the SIWS 26 may not be fully secure, this double check is necessary.

If the OC determines that the transaction data is invalid, the order is aborted (step 72).

Otherwise (step 74), the OC 20 adds a unique order number to the transaction data and sends them with approval to the SIU 24. The unique order number is used in every subsequent message concerning that order. The SIU 24 encrypts the transaction data using the Supplier's private key and sends the encrypted data and the Supplier's public ID number to the VC 40. It can be sent via the SIWS 26, directly via the Internet, or by any other communication method or system.

In step 76, the VC 40 uses the Supplier's public ID number to look up the Supplier's private key and decrypt the transaction data. Then the VC 40 does a preliminary validation (step 78). Typically this would involve checking that the Supplier exists and that the order would appear to be for goods or services provided by that supplier.

In step 80, if the preliminary validation fails, the VC 40 aborts the order.

Otherwise (step 82), the VC looks up the private key for Customer (using as an index the CPCN 16 or RTCN 22 that was included in the transaction data), uses the private key to encrypt the transaction data, and sends the encrypted data to the CIU 14 via the CSCIB 18 and the Internet. (The Customer e-mail address can entered with the order by the customer, added by the Supplier from its database, or taken by the VC 40 from the private key lookup table.

In step 84 the CIU 14 receives the transaction data, decrypts it, and displays the information to the Customer. Typically, this includes a list of products ordered, their prices, the payment method, and the total amount to be paid. From this point on, the price commitment of the Supplier is considered final.

In step 86, the Customer checks the transaction information and uses the CIU 14 keypad to confirm or reject the transaction. From this point on, the Customer's approval/disapproval of the transaction is considered final.

In step 88, the CIU 14 encrypts the Customer response using the Customer's private key and sends the response and the CPCN 16 to the VC 40.

In step 90, the VC 40 takes the CPCN 16 and looks up the Customer's private key, which it then uses to decrypt the response and to see what it is (step 92).

If the customer's response is negative, the order is aborted (94).

Otherwise (steps 96, 98), the VC 40 uses standard secure electronic banking methods to check the Customer's credit for the payment method that the Customer has selected.

If the VC 40 is unable to confirm the Customer's ability to pay (100), the transaction is aborted, otherwise (step 102), the VC 40 proceeds to debit the Customer's account and credit the Supplier account with the amount of the transaction.

The VC 40 encrypts a message confirming payment using the Supplier's private key and sends the encrypted message to the SIU 24.

In step 104, the SIU 24 decrypts the message and in step 106 checks to see whether it is positive (Customer paid). If he didn't pay (step 108), the transaction is aborted, otherwise (step 110), the SIU 24, sends the data to the OC 20, which checks the approved transaction against the original order (standard data integrity check) and supplies the Customer with the goods and/or services.

The present invention provides a novel design of a system that provides full protection against the theft of information via a communications network.. This design of the system for secure transactions via a communications network makes it particularly suitable for e-commerce transactions via the Internet. This is important for preventing unlawful access to Customer and/or supplier data and as a consequence promotes the growth of secure e-commerce.

It should be clear that the description of the embodiments and attached Figures set forth in this specification serves only for a better understanding of the invention, without limiting its scope as covered by the following Claims.

It should also be clear that a person skilled in the art, after reading the present specification could make adjustments or amendments to the attached Figures and above described embodiments that would still be covered by the following Claims.

CLAIMS

We claim:

1 A method for facilitating online commerce between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device, the method comprising the following steps:

a providing the customer with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device and having user input/output means, the customer's dedicated computing means communicating with the customer computing device; and

b providing the supplier with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device, the supplier's computing means communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing means; and

c requesting customer confirmation; and

d executing payment upon confirmation; and

e supplying goods or services.

2 A method as recited in claim 1, wherein the requesting customer confirmation step comprises the following steps:

a initially validating the customer order on the supplier's order-filling computing means;

b encrypting the order with supplier's private code and sending a payment request to the validating computing device;

c decrypting the order, encrypting with user's private code and sending to customer's dedicated computing means;

d decrypting the order and outputting it to the customer;

e the customer inputting his or her confirmation;

f encrypting the confirmation and sending to the validating computing device;

3 A method as recited in claim 1, wherein the executing payment upon confirmation step comprises the following steps:

a decrypting the customer confirmation;

b notifying the customer's payment provider to execute payment;

c receiving confirmation of payment from said payment provider;

d encrypting payment confirmation and sending to supplier's dedicated computing means;

4 A method as recited in claim 1, wherein the supplying goods or services step comprises the following steps:

a decrypting the payment confirmation;

b notifying supplier's order-filling computing means to execute order;

c filling order by providing goods or services to customer.

5 A method as recited in claim 1, wherein the supplier's order-filling computing means checks confirmed order against original order.

6 A method as recited in claim 1, wherein the method is carried out automatically.

7 A method as recited in claim 1, wherein the requesting customer confirmation step, the executing payment upon confirmation step, and the supplying goods or services step are all carried out online.

8 A method as recited in claim 1 carried out over the Internet.

9 A method as recited in claim 1, carried out over an intranet.

10 A method as recited in claim 1, wherein the transaction is initiated at an e-commerce Web site.

11 A method as recited in claim 1, wherein the method is carried out automatically.

12 A method as recited in claim 1, wherein the validating computing device maintains a copy of the transaction.

13 A method as recited in claim 1, wherein the validating computing device maintains a database about the transaction.

14 A method as recited in claim 1, wherein all encrypted messages for a given order have a unique identifier known and checked by the supplier's order-filling computing means.

15 A method as recited in claim 1, wherein the customer's dedicated computing means is a stand-alone device.

16 A method as recited in claim 1, wherein the customer's dedicated computing means is integrated into a remote control unit, the customer's computing device is a Web-enabled television set, and the two are connected via a bidirectional communications means.

17 A method as recited in claim 1, wherein the customer's dedicated computing means is an electronic commerce card;

18 A method as recited in claim 1, wherein the supplier's dedicated computing means is a stand-alone device.

19 A method as recited in claim 1, wherein the customer's dedicated computing means is provided with user access protection means.

20 A method as recited in claim 1, wherein the customer input means on the customer's dedicated computing means is touch-based, as in a keyboard, keypad, or touchscreen and appropriate software.

21 A method as recited in claim **1**, wherein the customer input means on the customer's dedicated computing means is voice-based, as in a microphone and voice recognition software.

22 A method as recited in claim **1**, wherein the means for output to the customer on the customer's dedicated computing means is display-based, as in an alpha-numeric or graphical display and appropriate software.

23 A method as recited in claim **1**, wherein the means for output to the customer on the customer's dedicated computing means is to a port, as in a parallel port to a printer.

24 A method as recited in claim **1**, wherein the means for output to the customer is to a printer integrated into the customer's dedicated computing means.

25 A method as recited in claim **1**, wherein the customer has a public identification code.

26 A method as recited in claim **1**, wherein the validating computing device provides the customer's dedicated computing means with an anonymous identification code.

27 At a customer conducting an online transaction, a method for handling an order confirmation request from a validating computing device, comprising the following steps:

a providing the customer with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device and having user input/output means, the customer's dedicated computing means communicating with the customer computing device;

b the dedicated computing means receiving an encrypted confirmation request from the validating computing device;

c decrypting the order and outputting it to the customer;

d the customer inputting his or her confirmation;

e encrypting the confirmation and sending to the validating computing device;

28 At a supplier conducting an online transaction, a method for working with a validating computing device and an order-filling computing means to confirm, bill, and fill a customer order, comprising the following steps:

a providing the supplier with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device, the supplier's computing means communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing means;

b initially validating the customer order on the supplier's order-filling computing means;

c encrypting the order with supplier's private code and sending payment request to the validating computing device;

d decrypting payment confirmation received from validating computing device;

e notifying supplier's order-filling computing means to execute order;

f filling order by providing goods or services to customer.

29 A method for facilitating online transactions between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device, the method comprising the following steps:

a providing the customer with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device and having user input/output means, the customer's dedicated computing means communicating with the customer computing device;

b providing the supplier with a dedicated computing means for security-critical parts of the transaction, the computing means having capabilities for encryption/decryption known only to the computing means and the validating computing device, the supplier's computing means communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing means;

c requesting customer confirmation, comprising the following steps:

i initially validating the customer order on the supplier's order-filling computing means;

ii encrypting the order with supplier's private code and sending a payment request to the validating computing device;

iii decrypting the order, encrypting with user's private code and sending to customer's dedicated computing means;

iv decrypting the order and outputting it to the customer;

v the customer inputting his or her confirmation;

vi encrypting the confirmation and sending to the validating computing device;

d executing payment upon confirmation, comprising the following steps:

i initially validating the customer order on the supplier's order-filling computing means;

ii decrypting the customer confirmation;

iii notifying the customer's payment provider to execute payment;

iv receiving confirmation of payment from said payment provider;

v encrypting payment confirmation and sending to supplier's dedicated computing means;

e and supplying the goods or services, comprising the following steps:

i decrypting the payment confirmation;

ii notifying supplier's order-filling computing means to execute order;

iii filling order by providing goods or services to customer.

30 A system for facilitating online transactions between a customer's computer device and a supplier's computing device, in cooperation with a validating computing device, the system comprising the following:

a a dedicated customer computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device and having user input/output device, the customer's dedicated computing device communicating with the customer computing device and programmed to receive an order confirmation request, decrypt the request, output the request to the user (customer), receive the customer's response (input) to the confirmation request, encrypt the customer response; and send the response to the validating computing device;

b a dedicated supplier computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device, the supplier's computing device communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing device and programmed to receive a customer order from the supplier's transaction site, encrypt an order and payment confirmation request, send the request to the validating computing device; receive order and payment confirmed message from the validating computing device, and notify the order-filling computing device to fill the order.

c the validating computing device being configured to receive an order and payment confirmation request from the dedicated supplier computing device, decrypt the request, encrypt an order confirmation request for the customer, send the request to the customer, receive the customer's response, decrypt the response, notify the customer's payment provider to execute payment, receive confirmation of payment from said payment provider; encrypt an order and payment confirmed message, and send said message to the dedicated supplier computing device.

31 A system for facilitating online commerce between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device, the system comprising the following steps:

a providing the customer with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device and having user input/output device, the customer's dedicated computing device communicating with the customer computing device; and

b providing the supplier with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device, the supplier's computing device communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing device; and

c requesting customer confirmation; and

d executing payment upon confirmation; and

e supplying goods or services.

32 A system as recited in claim 31, wherein the requesting customer confirmation step comprises the following steps:

a initially validating the customer order on the supplier's order-filling computing device;

b encrypting the order with supplier's private code and sending a payment request to the validating computing device;

c decrypting the order, encrypting with user's private code and sending to customer's dedicated computing device;

d decrypting the order and outputting it to the customer;

e the customer inputting his or her confirmation;

f encrypting the confirmation and sending to the validating computing device;

33 A system as recited in claim 31, wherein the executing payment upon confirmation step comprises the following steps:

a decrypting the customer confirmation;

b notifying the customer's payment provider to execute payment;

c receiving confirmation of payment from said payment provider;

d encrypting payment confirmation and sending to supplier's dedicated computing device;

34 A system as recited in claim 31, wherein the supplying goods or services step comprises the following steps:

a decrypting the payment confirmation;

b notifying supplier's order-filling computing device to execute order;

c filling order by providing goods or services to customer.

35 A system as recited in claim 31, wherein the supplier's order-filling computing device verifies that the confirmed order matches the original order.

36 A system as recited in claim 31, wherein the method is carried out automatically.

37 A system as recited in claim 31, wherein the requesting customer confirmation step, the executing payment upon confirmation step, and the supplying goods or services step are all carried out online.

38 A system as recited in claim 31, carried out over the Internet

39 A system as recited in claim 31, carried out over an intranet

40 A system as recited in claim 31, wherein the transaction is initiated at an e-commerce Web site.

41 A system as recited in claim 31, wherein the method is carried out automatically.

42 A system as recited in claim 31, wherein the validating computing device maintains a copy of the transaction.

43 A system as recited in claim 31, wherein the validating computing device maintains a database about the transaction.

44 A system as recited in claim 31, wherein all encrypted messages for a given order have a unique identifier known and checked by the supplier's order-filling computing device.

45 A system as recited in claim 31, wherein the customer's dedicated computing device is a stand-alone device.

46 A system as recited in claim 31, wherein the customer's dedicated computing device is integrated into a remote control unit, the customer's computing device is a Web-enabled television set, and the two are connected via a bidirectional communications device.

47 A system as recited in claim 31, wherein the customer's dedicated computing device is an electronic commerce card;

48 A system as recited in claim 31, wherein the supplier's dedicated computing device is a stand-alone device.

49 A system as recited in claim 31, wherein the customer's dedicated computing device is provided with user access protection device.

50 A system as recited in claim 31, wherein the customer input device on the customer's dedicated computing device is touch-based, as in a keyboard, keypad, or touchscreen and appropriate software.

51 A system as recited in claim 31, wherein the customer input device on the customer's dedicated computing device is voice-based, as in a microphone and voice recognition software.

52 A system as recited in claim 31, wherein the device for output to the customer on the customer's dedicated computing device is display-based, as in an alpha-numeric or graphical display and appropriate software.

53 A system as recited in claim 31, wherein the device for output to the customer on the customer's dedicated computing device is to a port, as in a parallel port to a printer.

54 A system as recited in claim 31, wherein the device for output to the customer is to a printer integrated into the customer device.

55 A system as recited in claim 31, wherein the customer has a public identification code.

56 A system as recited in claim 31, wherein the validating computing device provides the customer's dedicated computing device with an anonymous identification code.

57 At a customer conducting an online transaction, A system for handling an order confirmation request from a validating computing device, comprising the following steps:

a providing the customer with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device and having user input/output device, the customer's dedicated computing device communicating with the customer computing device;

b the dedicated computing device receiving an encrypted confirmation request from the validating computing device;

c decrypting the order and outputting it to the customer;

d the customer inputting his or her confirmation;

e encrypting the confirmation and sending to the validating computing device;

58 At a supplier conducting an online transaction, A system for working with a validating computing device and an order-filling computing device to confirm, bill, and fill a customer order, comprising the following steps:

a providing the supplier with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device, the supplier's computing device communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing device;

b initially validating the customer order on the supplier's order-filling computing device;

c encrypting the order with supplier's private code and sending payment request to the validating computing device;

d decrypting payment confirmation received from validating computing device;

e notifying supplier's order-filling computing device to execute order;

f filling order by providing goods or services to customer.

59 A system for facilitating online transactions between a customer's computing device and a supplier's computing device, in cooperation with a validating computing device, the method comprising the following steps:

a providing the customer with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device and having user input/output device, the customer's dedicated computing device communicating with the customer computing device;

b providing the supplier with a dedicated computing device for security-critical parts of the transaction, the computing device having capabilities for encryption/decryption known only to the computing device and the validating computing device, the supplier's computing device communicating with the supplier's computing device and, through a separate communications channel, with the supplier's order-filling computing device;

c requesting customer confirmation, comprising the following steps:

iv initially validating the customer order on the supplier's order-filling computing device;

v encrypting the order with supplier's private code and sending a payment request to the validating computing device;

vi decrypting the order, encrypting with user's private code and sending to customer's dedicated computing device;

vii decrypting the order and outputting it to the customer;

viii the customer inputting his or her confirmation;

ix encrypting the confirmation and sending to the validating computing device;

d executing payment upon confirmation, comprising the following steps:

i initially validating the customer order on the supplier's order-filling computing device;

ii decrypting the customer confirmation;

iii notifying the customer's payment provider to execute payment;

iv receiving confirmation of payment from said payment provider;

v encrypting payment confirmation and sending to supplier's dedicated computing device;

e and supplying the goods or services, comprising the following steps:

i decrypting the payment confirmation;

ii notifying supplier's order-filling computing device to execute order;

iii filling order by providing goods or services to customer.

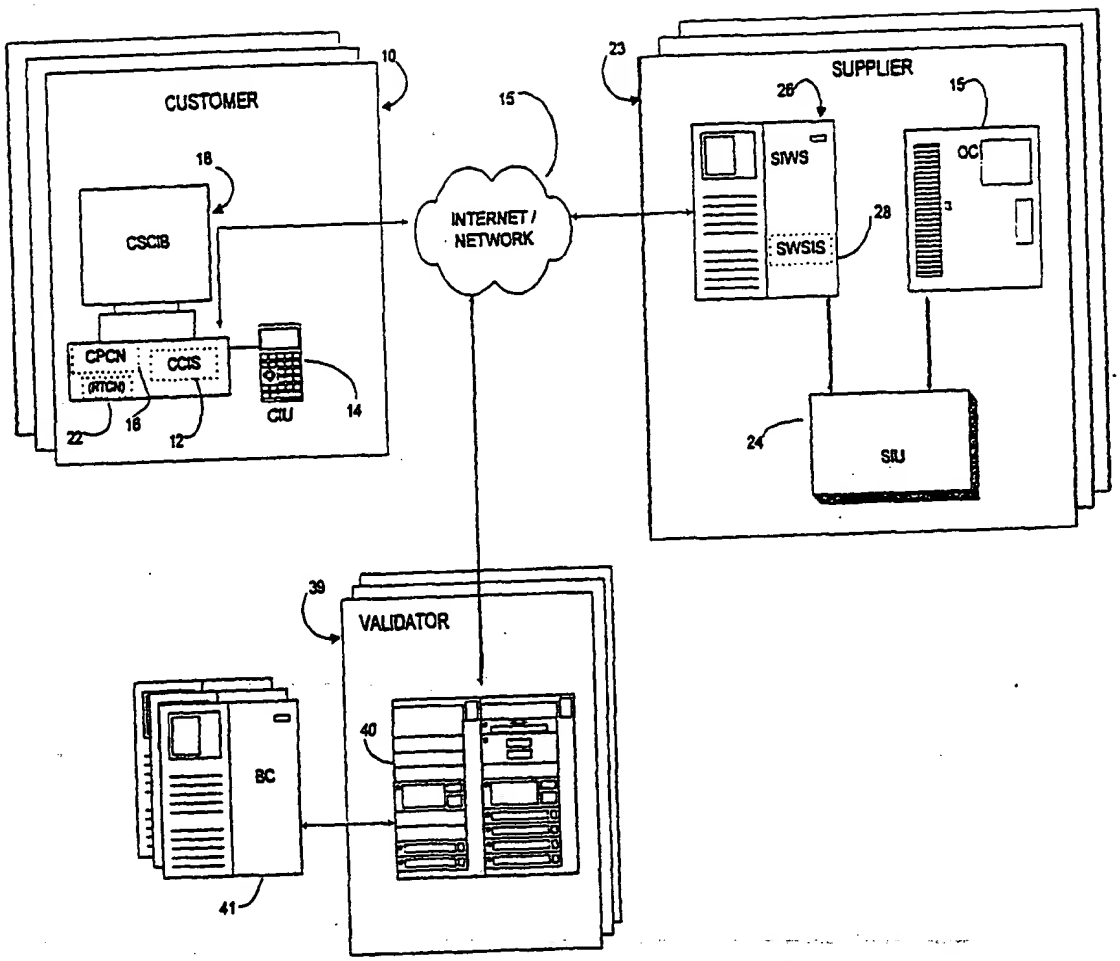

CUSTOMER
10
18
CSCIB
CPCN
(RTCM)
CCIS
22
16
12
CIU
14
15
INTERNET / NETWORK
23
SUPPLIER
26
SIWS
SWSIS
28
OC
24
SIU
39
VALIDATOR
40
BC
41

FIG. 1

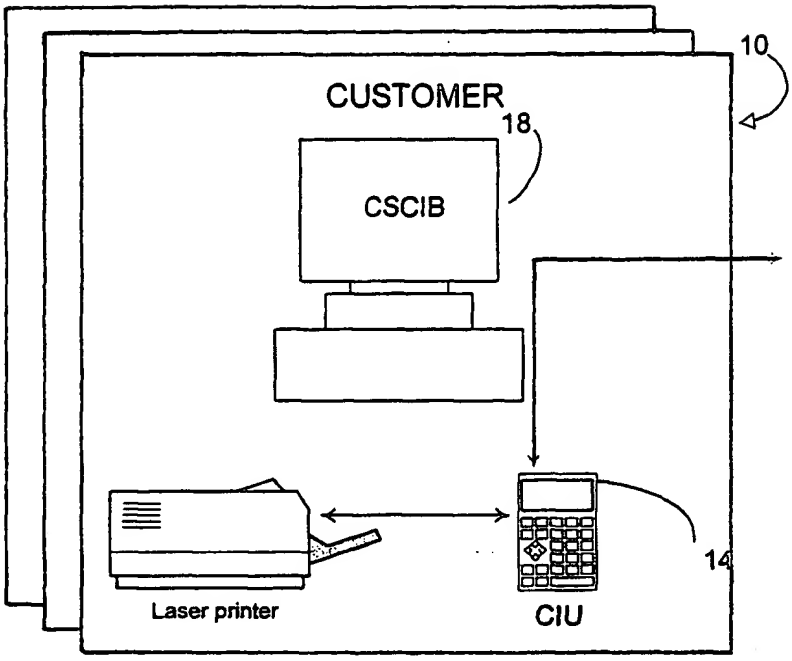

10
CUSTOMER
18
CSCIB
14
Laser printer
CIU

FIG. 2A

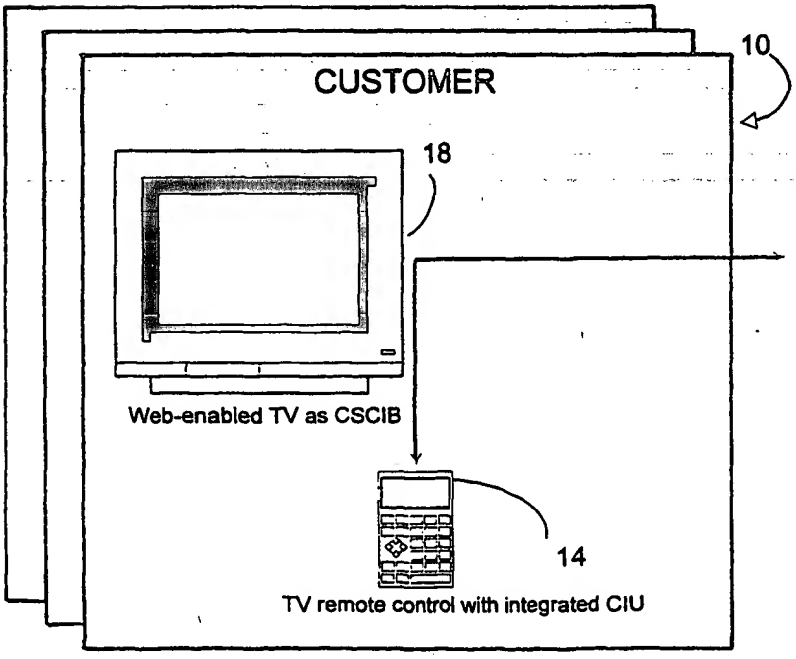

10
CUSTOMER
18
Web-enabled TV as CSCIB
14
TV remote control with integrated CIU

FIG. 2B

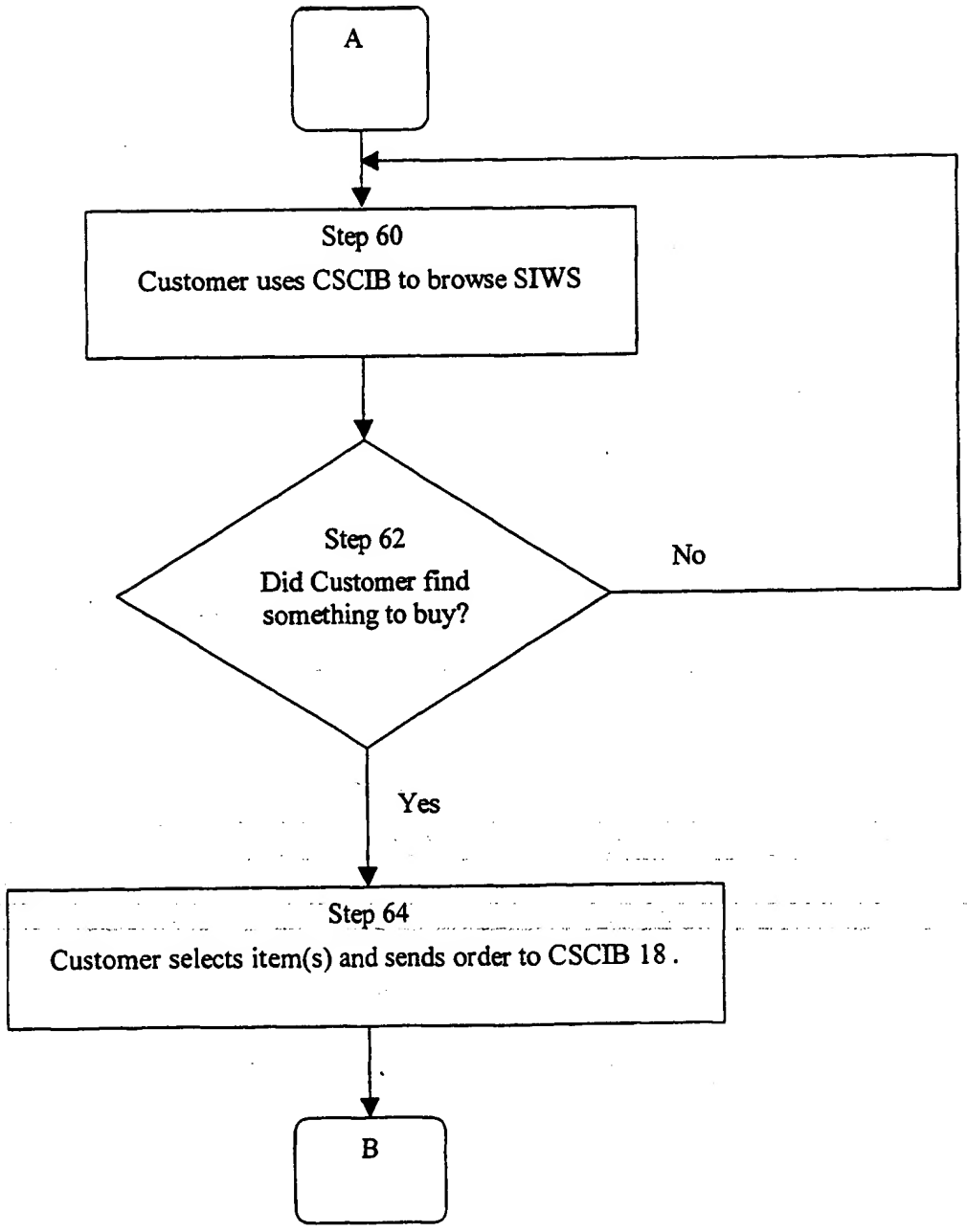

A
Step 60
Customer uses CSCIB to browse SIWS
Step 62
Did Customer find something to buy?
No
Yes
Step 64
Customer selects item(s) and sends order to CSCIB 18 .
B

FIG. 3A

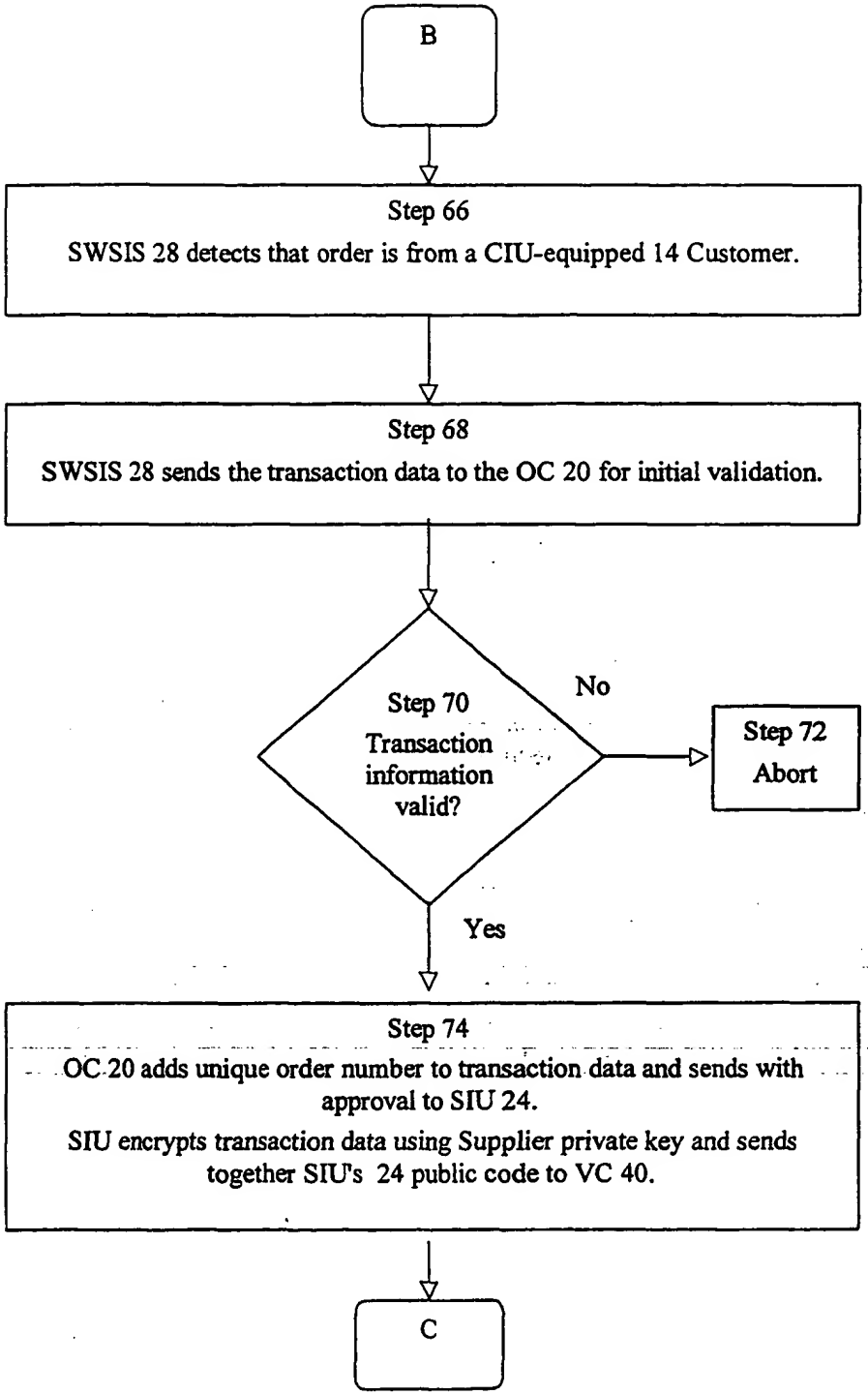

B
Step 66
SWSIS 28 detects that order is from a CIU-equipped 14 Customer.
Step 68
SWSIS 28 sends the transaction data to the OC 20 for initial validation.
Step 70
Transaction information valid?
No
Step 72
Abort
Yes
Step 74
OC 20 adds unique order number to transaction data and sends with approval to SIU 24.
SIU encrypts transaction data using Supplier private key and sends together SIU's 24 public code to VC 40.
C

FIG. 3B

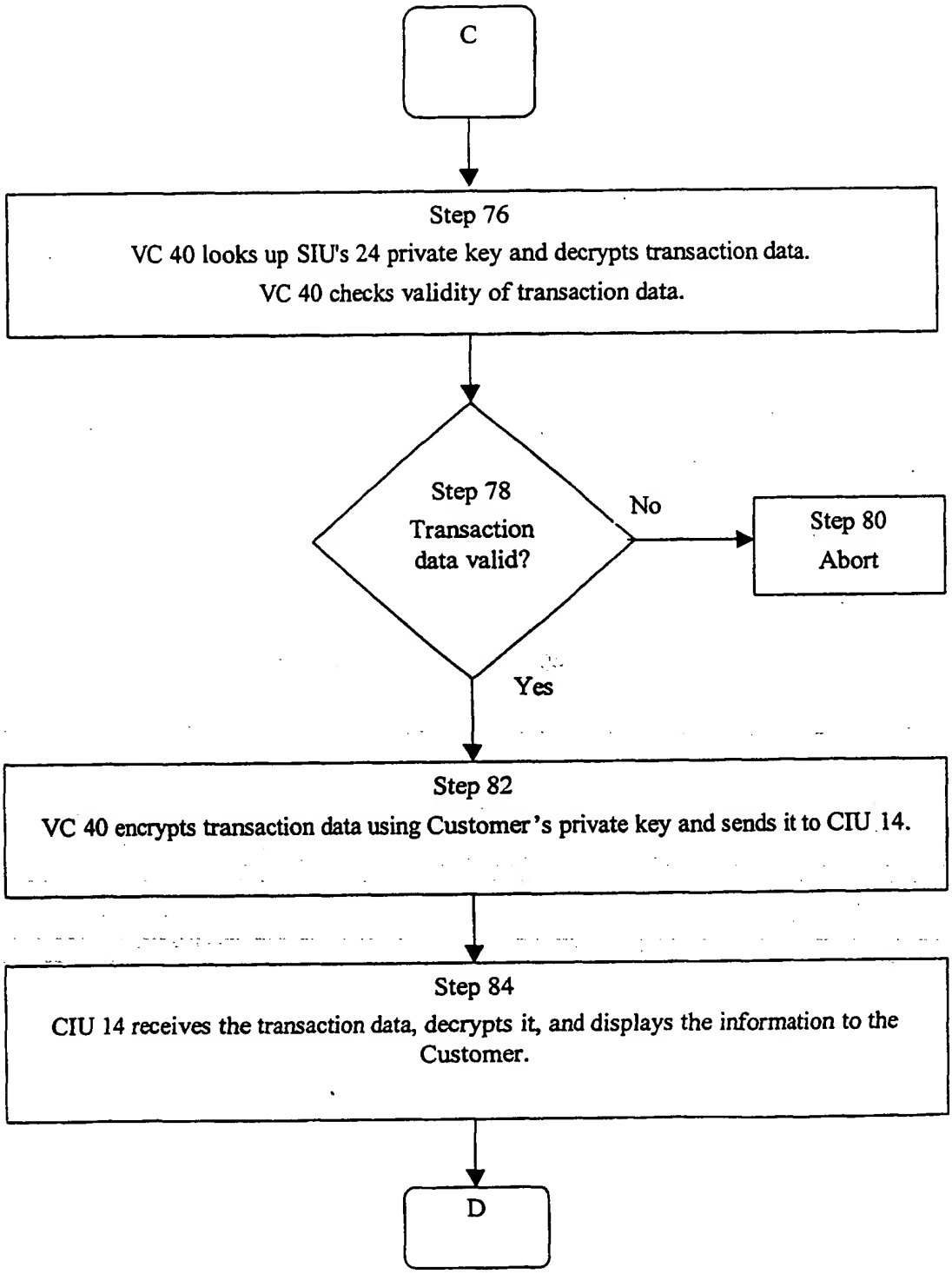

C
Step 76
VC 40 looks up SIU's 24 private key and decrypts transaction data.
VC 40 checks validity of transaction data.
Step 78
Transaction data valid?
No
Step 80
Abort
Yes
Step 82
VC 40 encrypts transaction data using Customer's private key and sends it to CIU 14.
Step 84
CIU 14 receives the transaction data, decrypts it, and displays the information to the Customer.
D

FIG. 3C

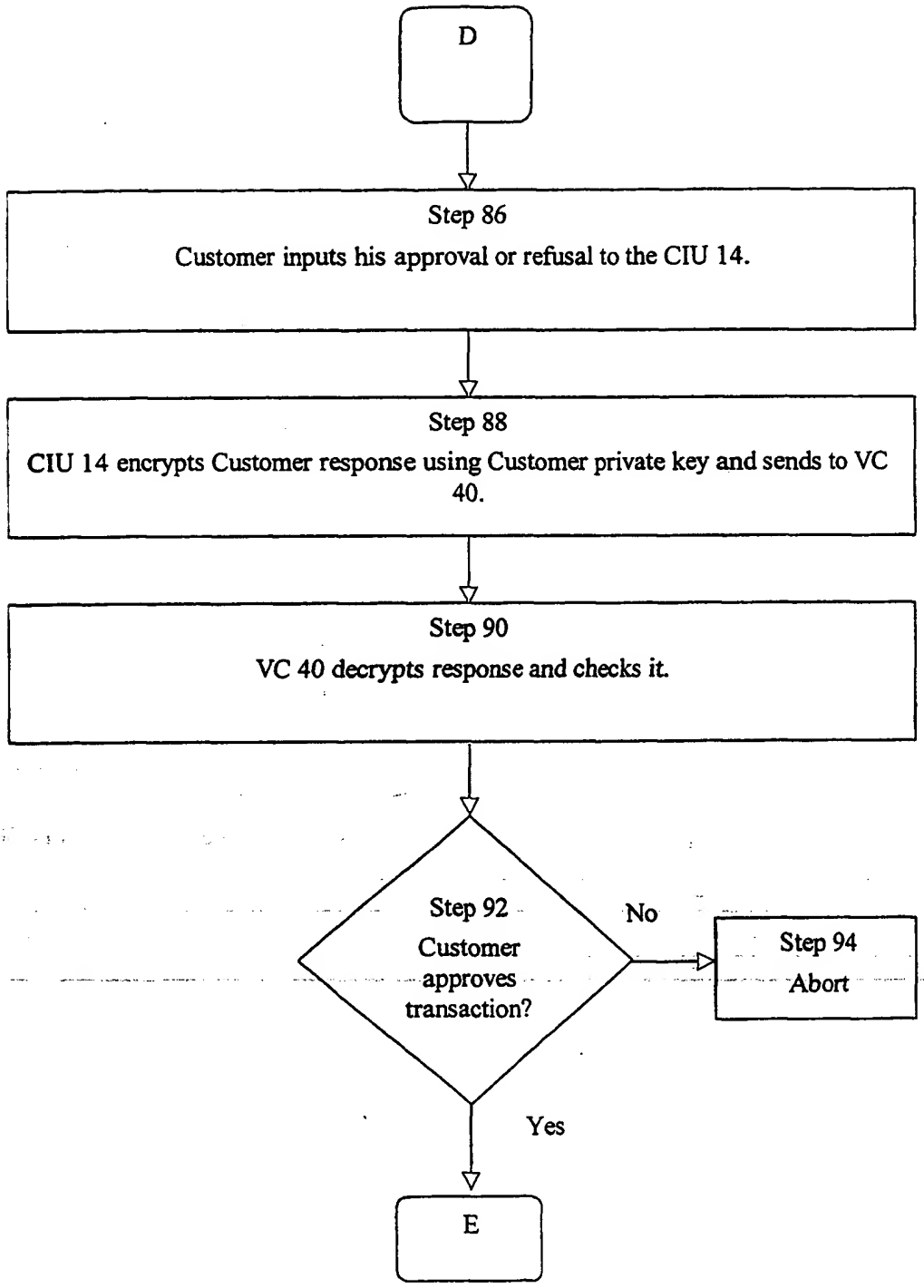

D
Step 86
Customer inputs his approval or refusal to the CIU 14.
Step 88
CIU 14 encrypts Customer response using Customer private key and sends to VC 40.
Step 90
VC 40 decrypts response and checks it.
Step 92
Customer approves transaction?
No
Step 94
Abort
Yes
E

FIG. 3D

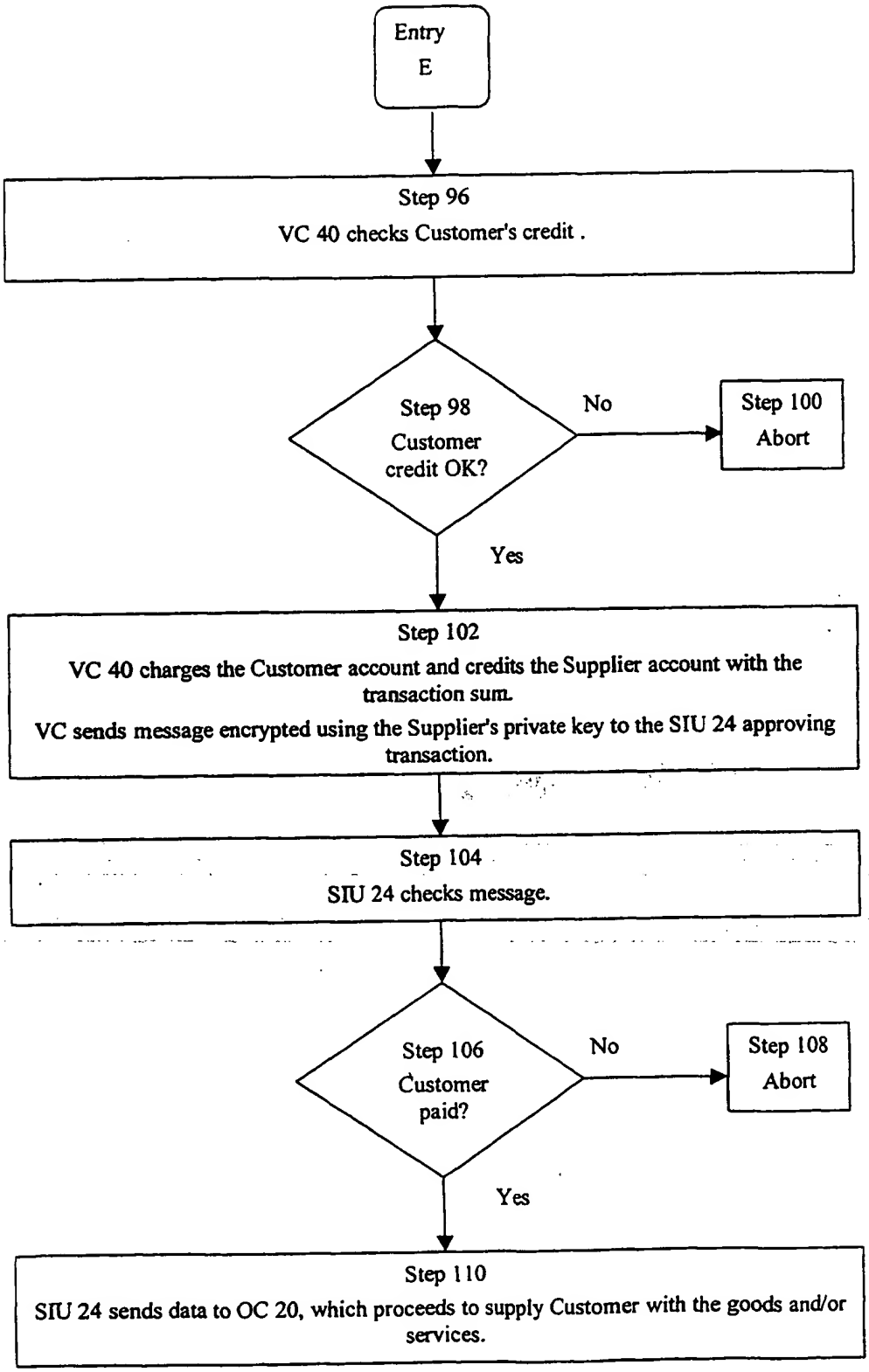

Entry
E
Step 96
VC 40 checks Customer's credit .
Step 98
Customer
credit OK?
No
Step 100
Abort
Yes
Step 102
VC 40 charges the Customer account and credits the Supplier account with the transaction sum.
VC sends message encrypted using the Supplier's private key to the SIU 24 approving transaction.
Step 104
SIU 24 checks message.
Step 106
Customer
paid?
No
Step 108
Abort
Yes
Step 110
SIU 24 sends data to OC 20, which proceeds to supply Customer with the goods and/or services.

FIG. 3E

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/92982 A3

(51) International Patent Classification[7]: H04K 1/00

(21) International Application Number: PCT/IL01/00489

(22) International Filing Date: 29 May 2001 (29.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/207,927 30 May 2000 (30.05.2000) US

(71) Applicant and
(72) Inventor: CASPI, Moshe [IL/IL]; No. 75, 99750 Zelafon (IL).

(74) Agent: MILLER - SIERADZKI ADVOCATES & PATENT ATTORNEYS; P.O. Box 6145, 31061 Haifa (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

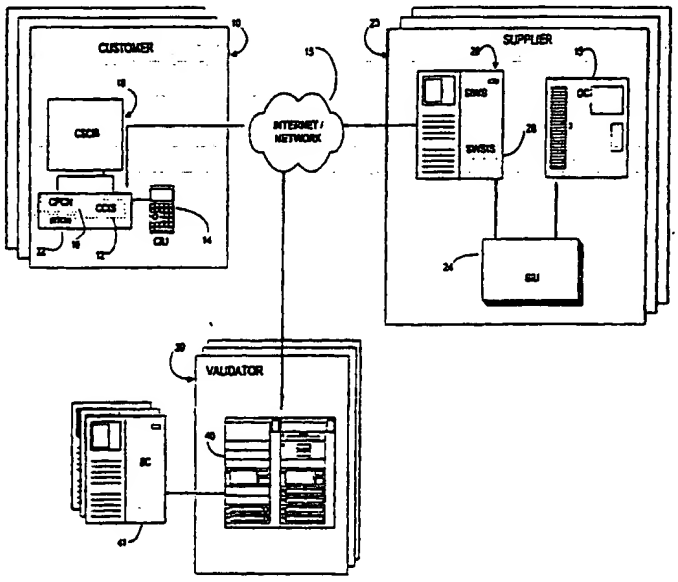
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
11 April 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD FOR SECURE TRANSACTIONS VIA A COMMUNICATIONS NETWORK



(57) Abstract: A method and a system for facilitating online commerce between a customer's computing device (18) and a supplier's computing device (15), in cooperation with a validating computing device (26). Security-sensitive input/output operations are carried out at each end of the transaction by dedicated computing means, one for the customer and one for the supplier. The dedicted customer computing means (18) is communication-connected (15) to the supplier's e-commerce server (26) and order-processing computer (15) via separate connections. Encrypted messages pass between the dedicated devices via a validating third party. The tasks handled are: requesting customer confirmation; executing payment upon confirmation and supplying goods or services.

WO 01/92982 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL01/00489

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04K 1/00

US CL : 705/65

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/64-67,75,77; 380/30; 713/155,200

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST, NPL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category°	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,677,955 A (DOGGETT et al). 14 October 1997, fig. 3, all, fig. 17a, all fig. 17b, allcol. 7 line 38-69, col. 8 lines 1-59.	1-4,7-20, 22-28, 31-50, 52-58
A	US 6,038,551 A (BARLOW et al.) 14 March 2000, Entire Document.	1-59
A,E	US 6,233,565 B1 A (LEWIS et al.) 15 May 2001, Entire Document.	1-59
A,P	US 6,105,008 A (DAVIS et al.) 15 August 2000, Entire Document.	1-59
A,E	US 2001/0039535 A1(TSIOUNIS et al.) 8 November, 2001, Entire Document.	1-59
A	US 5,590,197 A (CHEN et al.) 31 December 1996, Entire Document.	1-59

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

°	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
13 NOVEMBER 2001	
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PAUL E. CALLAHAN Telephone No. (703) 305-1336

Form PCT/ISA/210 (second sheet) (July 1998)☆